JOURNAL OF NUMBER THEORY 18, 342–349 (1984)

On p-Adic Zeros of Forms

W. DALE BROWNAWELL*

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802

Communicated by H. L. Montgomery

Received June 1, 1982; revised August 25, 1982

DEDICATED TO S. CHOWLA

Using the procedure of G. I. Arkhipov and A. A. Karatsuba (*Math. USSR-Izv.* **19** (1982), 321–340), their exponential lower bound on the number of variables possible for a form of degree d having only the trivial p-adic zero is sharpened.

I. INTRODUCTION

Motivated by considerations related to C. Tsen's work on central division algebras, E. Artin conjectured that every form $F(x_1,..., x_n)$ of degree d over a p-adic field $\mathbb{Q}_p$ must have a nontrivial zero provided only that $n > d^2$. (See [4, 5] for a fuller account of the history of the fruitful investigations into this question.) Artin's conjecture stood for some thirty years until Terjanian [7] produced a counterexample of degree four in 20 variables. Terjanian's construction was applied independently by Browkin [2], Samuel [8], and Schanuel [4] to produce counterexamples over each $\mathbb{Q}_p$. However, the technique could only construct forms with $n \leqslant d^3$ [6, p. 285].

Very recently Arkhipov and Karatsuba [1] have established the surprising fact that the number of variables in counterexamples is not even limited to polynomial growth with respect to the degree. By composing special forms with products of diagonal forms, they construct for each prime number p and $d > d_p$ a form $F(x_1,..., x_n)$ over $\mathbb{Z}$ of degree at most d having only the trivial zero in $\mathbb{Q}_p$ although

$$n > \exp\left(\frac{d}{(\log d)^2 (\log\log d)^3}\right).$$

* Research supported in part by the National Science Foundation.

0022-314X/84 $3.00

They argue by congruences modulo powers of p, calling a form $F(x_1,..., x_n)$ over $\mathbb{Z}$ *p-special* if there is some r (depending on F) such that every solution $(\alpha_1,..., \alpha_n)$ in $\mathbb{Z}^n$ of the congruence

$$F(x_1,..., x_n) \equiv 0 \pmod{p^r}$$

lies in $(p\mathbb{Z})^n$.

The purpose of this paper is to sharpen their result somewhat. For each prime number p, $\lambda_p(x)$ denotes a monotonically increasing positive function to be given explicitly later, but which is essentially the product of composites of logarithms of x. These functions grow so slowly that the series $\sum (n\lambda_p(n))^{-1}$ diverges (barely). By $\varepsilon(x)$ we denote the least number of levels in a tower such that

$$e^{e^{\cdots^{e}}} \geqslant x.$$

THEOREM. *For every prime number p there is an effectively calculable number d_p such that for every $d \geqslant d_p$, there is a p-special form $F(x_1,..., x_n)$ with*

$$\deg F \leqslant d,$$

$$n \geqslant \exp\left(\frac{d}{\lambda_p(d)(8p)^{\varepsilon(d)+1}}\right).$$

Since p-special forms have only the trivial zero in $\mathbb{Z}_p$ and, hence, in $\mathbb{Q}_p$, we deduce the following result:

COROLLARY. *For every prime number p and for every $d \geqslant d_p$, there is a form over $\mathbb{Z}$ of degree at most d in at least* $\exp(d/\lambda_p(d)(8p)^{\varepsilon(d)+1})$ *many variables which has only the trivial zero in $\mathbb{Q}_p$.*

Comparable results have been obtained independently by Lewis and Montgomery [5]. I have profited from discussions with R. G. Ayoub and R. Huff.

II. CONGRUENCES FOR DIAGONAL FORMS

The basic auxiliary results give lower bounds on the number of variables necessary to solve a rather large number of diagonal forms to a large power of p if the degrees of the forms are not too widely dispersed. As usual, the

treatment varies slightly according to whether our prime is even or odd. We consider the case $p = 2$ in detail.

BASIC EVEN LEMMA. *Let $R \in \mathbb{N}$. If the system of congruences*

$$\begin{aligned} x_1^{2j_1} + \cdots + x_n^{2j_1} &\equiv 0 \pmod{2^{2j_1}}, \\ &\vdots \\ x_1^{2j_R} + \cdots + x_n^{2j_R} &\equiv 0 \pmod{2^{2j_R}}, \end{aligned}$$

has a solution in $\mathbb{Z}^n$ with some entry odd, where

$$3R < j_1 < \cdots < j_R < 5R,$$

then

$$n \geqslant 2^{3R}.$$

Remark 1. Arkhipov and Karatsuba prove essentially that $\log n \gg R/\log R$, but mention improvements that would be strong enough for our purposes here.

Remark 2. More generally, if only $0 < L \leqslant j_1 < \cdots < j_R \leqslant U$ then the number of odd entries in a solution is a multiple of $2^{\min\{3R, 3L-U\}}$.

Remark 3. This lemma is nearly best possible in the light of results of Browkin [3] and Schanuel [6] which show that if n is known to be somewhat larger in such a system of congruences, then the system can indeed always be solved with some entries odd.

Proof of the Lemma. We may, without loss of generality, take *all* of the entries $\alpha_1, \ldots, \alpha_n$ in the solution to be odd and express them in the form $\alpha_i \equiv 5^{\beta_i} \bmod 2^{10R}$. When we set

$$f(t) = t^{\beta_1} + \cdots + t^{\beta_n},$$

our congruences become $f(5^{2j_r}) \equiv 0 \pmod{2^{2j_r}}$, $r = 1, \ldots, R$. Our object is to show that 2^{3R} divides $f(1)$, from which fact the lemma follows immediately.

To this end we represent $f(t)$ in a finite Newton interpolation polynomial

$$\begin{aligned} f(t) = a_0 &+ a_1(t - 5^{2j_R}) + a_2(t - 5^{2j_R})(t - 5^{2j_{R-1}}) \\ &+ \cdots + g(t)(t - 5^{2j_R}) \cdots (t - 5^{2j_1}) \end{aligned}$$

with $a_0, \ldots, a_{R-1} \in \mathbb{Z}$ and $g(t) \in \mathbb{Z}[t]$. For every nonzero integer n, let $v(n)$ denote the largest integer v with $2^v \mid n$.

Claim. For $r = 0,\ldots, R-1$, we have

$$3j_{R-r} - j_R - 3r \leqslant v(a_r).$$

The claim is established by induction on r with the case $r = 0$ true by the hypothesis that $f(5^{2j_R}) \equiv 0 \pmod{2^{2j_R}}$. If the claim is true for all $r < \rho$ $(\rho < R)$, then since $f(5^{2j_\rho}) \equiv 0 \pmod{2^{2j_\rho}}$, we find from the interpolation polynomial that

$$\min_{1 \leqslant r < \rho} \min\{v(a_r(5^{2j_{R-\rho}} - 5^{2j_R}) \cdots (5^{2j_{R-\rho}} - 5^{2j_{R-r+1}})), 2j_{R-r}\}$$
$$\leqslant v(a_\rho(5^{2j_{R-\rho}} - 5^{2j_R}) \cdots (5^{2j_{R-\rho}} - 5^{2j_{R-\rho+1}})).$$

If the minimum is, say, $2j_{R-r}$, then we estimate the right-hand side using the elementary facts that $v(m!) < m$ and $v(5^m - 1) = v(m) + 2$,

$$2j_{R-r} \leqslant v(a_\rho) + 3\rho + v((j_{R-\rho} - j_R) \cdots (j_{R-\rho} - j_{R-\rho+1}))$$
$$\leqslant v(a_\rho) + 3\rho + (j_R - j_{R-\rho}),$$

which is stronger than was claimed since $j_{R-\rho} < j_{R-r}$.

If the minimum occurs for the other type of term, we divide by the obvious common factor to obtain

$$v(a_r) \leqslant v(a_\rho) + v((5^{2j_{R-\rho}} - 5^{2j_{R-r}}) \cdots (5^{2j_{R-\rho}} - 5^{2j_{R-\rho+1}}))$$
$$\leqslant v(a_\rho) + 3(\rho - r) + (j_{R-r} - j_{R-\rho}),$$

which, by induction, gives the same inequality we obtained in the first case.

Thus the lemma is established once we notice that, since $g(t)$ has integral coefficients, the same sort of argument shows that $v(f(1))$ is at least

$$\min\{\min_{0 \leqslant r < R} \{v(a_r(1 - 5^{2j_{R-r+1}}) \cdots (1 - 5^{2j_{R-r+1}}))\}, v((1 - 5^{2j_R}) \cdots (1 - 5^{2j_1}))\}$$
$$\geqslant \min\{\min_{0 \leqslant r < R} \{3j_{R-r} - j_R\}, 3R\}.$$

The proof of the corresponding result for odd primes is completely analogous except that now one has a primitive root g and the elementary facts about ord are $v(m!) < m/(p-1)$ and $v(g^{(p-1)m} - 1) = v(m) + 1$.

BASIC ODD LEMMA. *Let $R \in \mathbb{N}$. If p is an odd prime and the system of congruences*

$$x_1^{(p-1)j_1} + \cdots + x_n^{(p-1)j_1} \equiv 0 \pmod{p^{(p-1)j_1}},$$
$$\vdots$$
$$x_1^{(p-1)j_R} + \cdots + x_n^{(p-1)j_R} \equiv 0 \pmod{p^{(p-1)j_R}},$$

with

$$R < j_1 < \cdots < j_R < 3R$$

has a solution in $\mathbb{Z}^n$ *with some entry not divisible by* p, *then*

$$p^R \leqslant n.$$

Remarks 1 and 3 apply to this lemma as well.

Remark 4. If, more generally, $0 < L \leqslant j_1 < \cdots < j_R \leqslant U$, then we find that the number of entries in a solution which are not divisible by p is a multiple of $p^{\min\{R, pL-U\}}$.

III. Minimal Degree of Special Forms

Fix for a moment a prime number p. The proof of the theorem will depend on a study of the growth of the function $\delta(n)$, which is defined as the least degree d of any p-special form in n variables. Consideration of norm forms for extensions of degree n over $\mathbb{Z}/p\mathbb{Z}$ shows that $\delta(n) \leqslant n$ for all n. The heart of the approach of Arkhipov and Karatsuba is the demonstration that $\delta(n)$ grows much more slowly than n. (The fact that $\delta(n) \leqslant \delta(n+1)$ follows on setting $x_{n+1} = 0$ in any p-special form of degree $\delta(n+1)$ in $n+1$ variables.)

The following remark will be useful in establishing the basic inequality for $\delta(n)$. Namely, if $F(x_1,..., x_n)$ is p-special then it is seen on successively dividing solutions by p, that for any $m > 0$ there is an M such that every solution of $F(x_1,..., x_n) \equiv 0 \pmod{p^M}$ has all entries divisible by p^m.

Let us now consider the case $p = 2$. For any integer $t > 1$ let $F(y_1,..., y_t)$ be a 2-special form of degree $\delta(t)$. Since F is 2-special, there is an $M > 0$ such that when $F(y_1,..., y_t) \equiv 0 \pmod{2^M}$, we must have

$$y_1 \equiv \cdots \equiv y_t \equiv 0 \pmod{2^{16t}}.$$

Consider the composite form $G(x_1,..., x_n)$ of degree $16t\delta(t)$ obtained by setting

$$y_j = S_{2(4t-j)} S_{2(4t+j)}, \qquad j = 0,..., t-1,$$

where $S_k = x_1^k + \cdots + x_n^k$ for any $k > 0$. From our definition of y_j, it follows that when $G(x_1,..., x_n) \equiv 0 \pmod{2^M}$ we have for each j that either

$$S_{8t-2j} \equiv 0 \pmod{2^{8t-2j}}$$

or else

$$S_{8t+2j} \equiv 0 \pmod{2^{8t+2j}}.$$

Thus by our fundamental lemma, if any x_1 is odd, we must have $n \geqslant 2^{3t}$. Consequently, if in our choice of diagonal forms S_k we hold n below this bound, we can be sure that in any solution to $G(x_1, ..., x_n) \equiv 0 \pmod{2^M}$, all entries must be even. As a result we know that for all $n < 2^{3t}$,

$$\delta(n) \leqslant 16t\delta(t).$$

Applying this conclusion inductively yields the next result once we extend the definition of δ to all of $\mathbb{R} > 1$ via $\delta(x) := \delta(\lfloor x \rfloor)$.

AN EVEN PROPOSITION. *For $p = 2$,*

$$\delta(n) < 16^{\varepsilon(n)}\lambda_2(n)$$

for all $n > 1$, where $\varepsilon(n)$ denotes the number of levels in the least exponential tower of e's greater than n, i.e.,

$$e^{e^{\cdot^{\cdot^{\cdot^{e}}}}} \geqslant n \qquad \text{and} \qquad \lambda_2(n) = \prod \prod \log^{(l)} n$$

is the product over all composites of the natural logarithm with $\log^{(l)} n > 1$.

Proof. For $n \leqslant 8$, trivially $\delta(n) \leqslant 8 = 8^{\varepsilon(2)}$. Now when $n \geqslant 8$ there is an integer $t \in \mathbb{N}$ with $8^{t-1} \leqslant n < 8^t$. Then

$$t \leqslant 1 + (\log_2 n)/3 < \log n.$$

Thus in this case we find by the paragraph above that

$$\delta(n) < 16t\delta(t) < 16(\log n)\,\delta(\log n),$$

and we are through by induction on $\varepsilon(n)$.

Remark 5. It is easily seen by the integral test that $\sum (n\lambda_2(n))^{-1}$ diverges while $\sum (16^{\varepsilon(n)} n\lambda_2(n))^{-1}$ converges. The corresponding remark applies to the following proposition as well.

AN ODD PROPOSITION. *For p an odd prime number,*

$$\delta(n) < (4(p-1))^{\varepsilon(n)}\,\lambda_p(n),$$

where $\delta(n)$ and $\varepsilon(n)$ are defined as above and $\lambda_p(n)$ is defined as the product $\prod \prod l_p^{(k)}(n)$ over all composites of $l_p(x) := 1 + \log_p x$ with value greater than 1 at $x = n$.

The result is established as for $p = 2$, but the basic underlying inequality for odd p is that

$$\delta(n) < 4(p-1)(1+\log_p n)\,\delta(1+\log_p n).$$

IV. Proof of the Theorem

The theorem follows simply by applying first the underlying inequality for $\delta(n)$ and then the estimates of the preceding propositions with n chosen as

$$n = \left[\exp\left(\frac{d}{(8p)^{\varepsilon(d)+1}\lambda_p(d)}\right)\right] \geqslant 8.$$

Then

$$\begin{aligned}\delta(n) &< (8p)\,l_p(n)\,\delta\left(\frac{d}{(8p)^{\varepsilon(d)+1}\lambda_p(d)}\right)\\ &< 8pl_p(n)\,\delta(d)\\ &< 8p\left(\frac{d}{(8p)^{\varepsilon(d)+1}\lambda_p(d)}\right)\delta(d), \qquad \text{when} \quad n \geqslant 8,\\ &< d,\end{aligned}$$

where for the sake of uniform notation we have set $l_2(x) := \log x$. Thus the constant d_p is determined by the constraint that n always be at least 8.

To the interesting conjectures on the structure of counterexamples to Artin's conjecture found in [1, 4] should be added S. Lang's question about the growth of n with respect to the degree for noncomposite special forms.

Acknowledgment

The author is indebted to J. Browkin for indicating the appropriate reference [3]. His recent related work, On systems of congruences, to appear in *Bull. Acad. Polon. Sci.*, gives examples of polynomials over $\mathbb{Z}$ which vanish only at $(0,\ldots,0)$ over $\mathbb{Q}_p$ although $n \gg dc^d$.

Note added in proof. In a recent paper, On a problem in the theory of equations, *Uspechi Mat. Nauk* **37** (1982), 161–162, Arkhipov and Karatsuba have announced an improvement of their basic results in [1]. More precisely, the actual formulation they use puts the strength of the results between those of [5] and the present paper.

Y. Alemu has generalised these considerations to forms over finite extensions of $\mathbb{Q}_p$ in his thesis, Warsaw University, 1983.

REFERENCES

1. G. I. ARKHIPOV AND A. A. KARATSUBA, On the local representation of zero by a form, *Izv. Akad. Nauk SSSR Ser. Mat.* **45** (1981), 948–961; translated in *Math USSR-Izv.* **19** (1982), 231–240.
2. J. BROWKIN, On forms over p-adic fields, *Bull. Acad. Polon. Sci.* **14** (1966), 489–492.
3. J. BROWKIN, On zeros of forms, *Bull. Acad. Polon. Sci.* **17** (1969), 611–616.
4. M. J. GREENBERG, "Lectures on Forms in Many Variables," Benjamin–Cummings, Reading, Mass., 1969.
5. D. J. LEWIS AND H. L. MONTGOMERY, On zeros of p-adic forms, *Michigan Math. J.* **30** (1983), 83–87.
6. S. H. SCHANUEL, An extension of Chevalley's theorem to congruences modulo prime powers, *J. Number Theory* **6** (1974), 284–290.
7. G. TERJANIAN, Un contre-example à une conjecture d'Artin, *C. R. Acad. Sci. Paris Ser. I Math.* **262** (1966), 612.
8. G. TERJANIAN, Formes p-adiques anisotropes, *J. Reine Angew. Math.* **313** (1980), 217–220.